AMENDMENTS TO THE CLAIMS

Claim 1 (Presently Amended): A device for calculating a result of a modular exponentiation within an asymmetrical cryptosystem, n being a modulus, d being an exponent and a private key of the asymmetrical cryptosystem, ~~and~~ c being a quantity to be subjected to the modular exponentiation, and, as a result, a quantity m is obtained which equals the modular exponentiation of c with the private key d as an exponent, comprising:

means for calculating a first auxiliary quantity dp, wherein the means for calculating a first auxiliary quantity is formed to calculate the first auxiliary quantity dp ~~is defined~~ as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number, and wherein mod represents a modulo operation;

means for calculating a second auxiliary quantity dq, wherein the means for calculating a second auxiliary quantity is formed to calculate the second auxiliary quantity dq according to the following equation~~is defined as follows~~:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

means for generating a random number (IRND);

means for generating a third auxiliary quantity dp′, wherein the means for generating a third auxiliary quantity dp′ is formed to calculate the third auxiliary quantity according to the following equation ~~is defined as follows~~:

$$dp' = IRND \times (p - 1) + dp,$$

wherein IRND is a random number generated by the means for generating a random number, and wherein dp is the first auxiliary quantity calculated by the means for calculating a first auxiliary quantity;

means for generating a fourth auxiliary quantity dq′, wherein dq′ is defined according to the following equation~~as follows~~:

$$dq' = IRND \times (q - 1) + dq,\cancel{;}$$

wherein IRND is the random number generated by the means for generating a random number, and wherein dq is the second auxiliary quantity calculated by the means for calculating a second auxiliary quantity;

means for generating a safety parameter T;

means for generating a fifth auxiliary quantity Mp, wherein the means for generating a fifth auxiliary quantity is formed to calculate the fifth auxiliary quantity Mp according to the following equation~~is defined as follows~~:

$$Mp = c^{dp'} \bmod (pT),\cancel{;}$$

wherein T is a safety parameter generated by the means for generating a safety parameter, and wherein dp’ is the third auxiliary quantity calculated by the means for calculating a third auxiliary quantity;

means for generating a sixth auxiliary quantity Mq, wherein the means for generating a sixth auxiliary quantity is formed to calculate the sixth auxiliary quantity Mq according to the following equation~~is defined as follows~~:

$$Mq = c^{dq'} \bmod (qT),\cancel{;} \text{ and}$$

wherein T is the safety parameter generated by the means for generating a safety parameter, and wherein dq' is the fourth auxiliary quantity calculated by the means for calculating a fourth auxiliary quantity;

means for calculating a seventh auxiliary quantity H7, wherein the means for calculating the seventh auxiliary quantity is formed to calculate the seventh auxiliary quantity H7 according to the following equation:

$$H7 = Mp \times Mq \bmod T,$$

wherein T is the safety parameter T generated by the means for generating a safety parameter, wherein Mp is the fifth auxiliary quantity calculated by the means for generating a fifth auxiliary quantity, and wherein Mq is the sixth auxiliary quantity calculated by the means for generating a sixth auxiliary quantity;~~and~~

means for calculating an eighth auxiliary quantity H8, wherein the means for calculating an eighth auxiliary quantity H8 is formed to calculate the eighth auxiliary quantity H8 according to the following equation:

$$H8 = c^{(dp'+dq' \bmod (T-1))} \bmod T,$$

wherein T is the safety parameter T generated by the means for generating a safety parameter, wherein dp' is the third auxiliary quantity calculated by the means for generating a third auxiliary quantity, and wherein dq' is the fourth auxiliary quantity calculated by the means for generating a fourth auxiliary quantity;~~and~~

means for comparing the seventh auxiliary quantity H7 and the eighth auxiliary quantity H8, wherein the means for comparing is arranged to indicate an error if the seventh and eighth auxiliary quantities are different; and

means for calculating the result of the modular exponentiation m in case no error has been indicated, wherein the means for calculating is formed to calculate the result m according to the following equation ~~is defined as follows~~:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q,$$

wherein Mp is the fifth auxiliary quantity calculated by the means for generating a fifth auxiliary quantity, and wherein Mq is the sixth auxiliary quantity calculated by the means for generating a sixth auxiliary quantity.

Claims 2 and 3 (Deleted)

Claim 4 (Presently Amended): The device according to claim 1, being provided for an RSA decryption or RSA signature, m being a plain text message, d being a ~~secret~~ private key and c being an encrypted message.

Claim 5 (Deleted)

Claim 6 (Presently Amended): The device according to claim ~~5~~1, wherein the safety parameter T is a prime number.

Claim 7 (Presently Amended): The device according to claim ~~3~~1, wherein the safety parameter T is small compared to the first prime number p and the second prime number q, respectively.

Claim 8 (Presently Amended): A method for calculating a result of a modular exponentiation within an asymmetrical cryptosystem on a data processing device, n being a modulus, d being an exponent and a private key of the asymmetrical cryptosystem,~~and~~ c being a quantity to be subjected to the modular exponentiation, and, as a result, a quantity m is obtained which equals the modular exponentiation of c with the private key d as an exponent, comprising the following steps:

calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number;

calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

providing a random number (IRND);

generating a third auxiliary quantity dp′, wherein dp′ is defined as follows:

$$dp' = IRND \times (p - 1) + dp;$$

generating a fourth auxiliary quantity dq′, wherein dq′ is defined as follows:

$$dq' = IRND \times (q - 1) + dq;$$

generating a safety parameter T;

generating a fifth auxiliary quantity Mp, wherein the fifth auxiliary quantity Mp is defined as follows:

$$Mp = c^{dp'} \bmod (pT);$$

generating a sixth auxiliary quantity Mq, wherein the sixth auxiliary quantity Mq is defined as follows:

$$Mq = c^{dq'} \bmod (qT);$$ ~~and~~

calculating a seventh auxiliary quantity H7, wherein the seventh auxiliary quantity is defined as follows:

$$H7 = Mp + Mq \bmod T;$$

calculating an eighth auxiliary quantity H8, wherein the eighth auxiliary quantity H8 is defined as follows:

$$H8 = c^{(dp'+dq' \bmod (T-1))} \bmod T;$$

comparing the seventh auxiliary quantity H7 and the eighth auxiliary quantity H8;

indicating an error if the seventh and eighth auxiliary quantities are different; and

in case no error has been indicated, calculating the result of the modular exponentiation m, wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

Claim 9 (Deleted)